

TRANSFORMING NETWORK MANAGEMENT FOR THE FUTURE ARMY NETWORKS¹

Cho-Yu Jason Chiang* and Ritu Chadha
Telcordia Technologies
Piscataway, NJ 08854

Scott Newman* and Richard Lo
U.S. Army CERDEC
Fort Monmouth, NJ 07703

ABSTRACT

Network management has been used in daily operations for decades to maintain Army networks. With the inclusion of Mobile Ad hoc NETWORKs (MANETs) as tactical networks, we believe that the role and function of network management need adjustment. MANETs can provide the agility required by the future Army force; however, their topology will not be static, their wireless radio connectivity will not be stable, and their bandwidth capacity will not be abundant. Given that several ongoing programs including FCS, WIN-T and JTRS are jointly shaping the outlook of the future Army tactical networks with MANETs, it is imperative to ensure that the future Army networks will be integrated seamlessly so that they can deliver desirable communications performance to support network centric warfare. We envision that network management will play a key role in ensuring communications performance. Since network centric warfare will require the highest possible performance from the networks, *the focus of network management must transition from maintaining network operations to providing optimal communications services*. In this paper, we describe the issues and challenges in providing seamless communications services for the future Army networks, and discuss the path forward for supporting the vision of network centric warfare by means of transforming network management.

1. INTRODUCTION

Network management has been used in daily operations for decades to maintain Army networks. The current practice requires that network administrators manually configure networks to enable network operations. Network administrators use either a command line interface or GUI of management software to configure network devices; they must possess expertise to configure, verify and analyze network configurations. For a brigade-sized network, it could take days or even weeks for the entire network to be fully operational. The main function that the existing network management software provides is to monitor and collect the status of networks. Typically the status of networks in a region is collected at

a Network Operation Center (NOC). After networks start operations, network administrators at the NOCs monitor the status of the networks, make administrative decisions and take necessary actions when networks do not meet the operational requirements.

The Army networks are going through a renovation process to include the latest technologies to meet the future war-fighting needs. Several ongoing programs including FCS [PM FCS, 2006], WIN-T [PM WIN-T, 2006] and JTRS [JTRS JPEO, 2006] are jointly shaping the future Army tactical networks. By including a multitude of emerging technologies in these programs, the future tactical networks will become more versatile, rapidly deployable, and can be set up on demand. The ultimate goal of this renovation is that the modernized Army networks will support DoD's vision of network centric warfare. In essence, network centric warfare means that warfighters at all echelons will be able to access information they need in near real time anywhere and anytime. Since information is provided to warfighters by C2 applications, it is important to ensure that the future Army networks will deliver desirable performance to C2 applications from the standpoint of warfighters.

Among the many emerging technologies that will be included in the future Army networks, both FCS and WIN-T programs use Mobile Ad hoc NETWORKs (MANETs) to achieve the agility required by the future Army force. Alongside these flagship acquisition programs, research objectives including policy-based network management (DRAMA, [Chadha et al, 2005a]) and mission-oriented network planning (DYMINION, [Chiang et al, 2006b]) 6.2/6.3 R&D programs¹ have been initiated by the U.S. Army CERDEC in the past years. The ultimate goal of these programs is to integrate MANETs into the Global Information Grid (GIG) and

¹ The research reported in this document/presentation was performed in connection with contract number DAAD19-01-C-0062 with the U.S. Army Research Laboratory. The views and conclusions contained in this document are those of the authors and should not be interpreted as presenting the official policies or position, either expressed or implied, of the U.S. Army Research Laboratory, or the U.S. Government unless so designated by other authorized documents. Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 NOV 2006		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Transforming Network Management For The Future Army Networks				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Telcordia Technologies Piscataway, NJ 08854				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES See also ADM002075., The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 8	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

adequately support the vision of network centric warfare. According to the DoD's report to the Congress [DoD, 2001], "Network centric warfare has the potential to increase warfighting capabilities by orders of magnitude." Its aim is to quickly supply war-fighters at all echelons with information useful for them to gain a decisive edge over enemies. Again, as stated in [DoD, 2001], "Network centric warfare represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner."

To achieve the vision of network centric warfare, the GIG is needed as an "organizing and transforming construct for managing information technology (IT) throughout the DoD" [DoD, 2004]. "The GIG vision is to empower users through easy access to information anytime and anyplace, under any condition, with attendant security. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. The goal is to increase the net-centricity of warfighter, business, intelligence, DoD enterprise management, and enterprise information environment management operations by enabling increased reach among the GIG users, increased richness in the information and expertise that can be applied to supporting operational decisions, increased agility in rapidly adapting information and information technology to meet changing operational needs, and increased assurance that the right information and resources to do the task will be there when and where it is required."

As the underlying framework for the future Army tactical networks, MANETs must be seamlessly integrated into the GIG to support network centric warfare. MANETs offer unprecedented advantages over conventional networks in terms of deployment efficiency and network coverage. However, based on our experience gained from executing the DRAMA and DYMINION programs, we consider it a true challenge to accomplish seamless integration, mainly due to the dynamicity of MANETs. As compared to the conventional GIG networks, MANETS are much more dynamic because (i) they do not require any fixed infrastructure; (ii) they use wireless radios rather than error-free fibers/cables as links between nodes; (iii) their network topologies change over time due to node movement and node failure. As a result, MANET's link connectivity is not stable, their radio link bandwidth fluctuates, and most importantly, the overall bandwidth capacity of a MANET as a whole is only a fraction of the maximum bandwidth of a single wireless radio link [Li, et al, 2001][Agarwal and Kumar, 2004]. This can be mainly attributed to wireless media contention and hidden terminal problems [Fullmer and Garcia-Luna-Aceves, 1997].

The lack of abundant bandwidth in MANETs will affect the overall communications effectiveness in the GIG. With the inclusion of MANETs, a simplified view of the future Army networks is as follows: the DoD/Army Internet provides the high-speed backbone network; satellite and long-range radio networks connect the backbone network to regional WIN-T networks, which connect to FCS networks providing communications services to frontline warfighters. Since the end points of a communication session may not be in the same segment of the GIG networks, e.g., a platoon warfighter accessing information hosted by a web server at Pentagon, it is important to ensure information will be delivered promptly, regardless of the number of network boundaries it needs to traverse. Although this is what Internet offers today, it does not include MANETs. When at least one of the communicating end points is located in a MANET, the issue of lack of bandwidth in MANETs, among others related to interconnecting the GIG with MANETs, will have significant impact on the ability to achieve the vision of network centric warfare.

Our view is that the key to tackling the foreseeable network integration challenges lies in transforming network management. The concept of network management should transition from *maintaining network operations* to *providing the optimal communications services*. This fundamental change of philosophy is the basis of our vision of transforming network management, and it has a profound impact. By following this vision, network management functions must assure that networks will deliver the best possible performance to C2 applications, rather than simply monitor and report whether networks are up and running. Furthermore, they must do so disregarding that the demands of applications may shift and network conditions may change. We must automate both network management and network planning as much as possible to assure that networks will always function effectively, even in dynamic and bandwidth-constrained environments.

The rest of this paper is organized as follows. In Section 2, we list the foreseeable issues and challenges that will be encountered when interconnecting the GIG with MANETs to support network centric warfare. In Section 3 we discuss prior art that was applied to resolve or alleviate issues similar to some of those for the future Army networks. In Section 4, we present our thinking on transforming network management, discuss recent research results, ongoing efforts, and a work plan for tackling the issues and challenges listed in Section 2. We present a possible path forward for transforming network management for the future Army network in Section 5, before concluding this paper.

2. ISSUES AND CHALLENGES

As mentioned earlier, we envision that network management will have to play a key role in enabling tomorrow's networks to meet expectations. The reason is straightforward—future Army tactical networks probably will not have abundant resources (primarily bandwidth) to meet the demands of network centric warfare. Therefore, prudent management of the limited resources to optimize their utilization becomes critical. As custom network management systems are being built for FCS and for WIN-T, the following questions arise: Will the new and existing network management systems provide sufficient and coherent functionality for managing tomorrow's tactical networks? What is path forward for network management?

To answer the above questions, we will first reflect upon what network management needs to accomplish for the future Army networks. To support network centric warfare, the future Army networks need to deliver the needed information to warfighters at all echelons in near real time. The focus, therefore, is on the timely delivery of information to warfighters using limited resources. Based on this reasoning, the major issues and challenges can be classified into the following categories: resource management in tactical networks, information transport across networks, automation and optimization of network operations, and coordination between network management systems. We elaborate on each of the issues and challenges below.

2.1 Resource management in tactical networks

As compared to conventional networks with fixed and stable link connections, the future tactical networks pose much greater management challenges. For example, FCS networks will be managed by a policy-based network management system. We therefore need to answer the following questions: How do we automate the generation of, or assist in the manual generation of network management policies? How do we manage QoS more effectively end-to-end? How do we further reduce human administration needs beyond FCS requirements? Another major issue for FCS networks is the use of SOSCOE, which is the common communications underlay for all applications. We need to investigate whether (i) SOSCOE can handle packets requiring the reliable transport provided by TCP but without the performance degradation of TCP within FCS networks and across the boundary of FCS networks; and (ii) SOSCOE should be managed by the FCS network management system as well, given that SOSCOE can be regarded as a part of the FCS network stack. And if so, how? To summarize, we must make better use of the available resources—both manpower and network bandwidth—to manage the future

tactical networks that are much more challenging to manage than conventional networks.

2.2 Information transport across networks

The Army network consists of heterogeneous networks and each of the networks has distinct characteristics. For example, bandwidth capacity and topology stability are expected to be excellent in the backbone network, but are expected to be dynamic and unstable in tactical networks. Since one size does not fit all, we are bound to design different solutions to the same problem for different networks. As a result, we need moderation and coordination approaches to smooth out the issues that arise when information with different transport requirements must transit through multiple networks having different characteristics in the areas of QoS, security, information assurance, etc. For example, FCS and WIN-T networks employ different QoS control mechanisms. It is important to ensure that the traffic that has been assured of a certain degree of QoS will receive the assured service end to end, regardless of the number of network boundaries that the traffic needs to transit across. Since communications sessions could take place between two nodes anywhere in the Army network, we need to make sure that the resource management on both sides will be coordinated by their respective network management systems.

2.3 Automation and optimization of network operations

Past research on MANETs has been focused mostly on enabling technologies such as radios, media access, routing, etc. With the coming of age of these networks, a grand challenge has emerged: *how do we automate both network management and network planning to assure that networks will function effectively in dynamic and possibly bandwidth-constrained environments?*

There are two areas where automation is needed. The first area arises from the dynamic nature of tactical networks, where the complexity of MANETs calls for the use of sophisticated software to replace manpower; the second area arises from the emerging requirements for supporting mission-oriented network operations, of which the aim is to optimize network performance based on specific communications needs of different types of missions.

2.4 Coordination between network management systems

The various types of networks that collectively provide communications services to the future Army force must collaboratively accomplish common objectives.

As shown in Fig. 1, the future Army networks will be managed by multiple network management systems. The questions to answer include: How do we specify common objectives and commander's intent? How should these objectives and intent be translated to different policies for different networks? Besides, since the policy-based network management paradigm has been adopted by both FCS and WIN-T, we need to answer the following questions: How do we know whether WIN-T policies and FCS policies are consistent with each other? If they are not, how do we make them consistent? How do we identify and resolve policy conflicts within the same type of network and between different types of networks? Is it beneficial and is it possible to have a unified policy framework for managing the entire Army network?

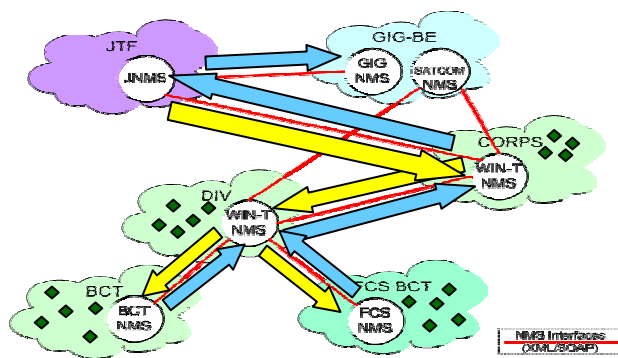


Fig. 1. An illustration of multiple network management systems in the future Army networks

3. PRIOR ART

In this section, we describe prior art that was conceived to resolve or relieve Internet problems similar to some of those for the future Army networks. We also discuss under each topic the limitations of prior art if it were to be applied directly to the future Army networks.

3.1 Content distribution management

As pointed out earlier, the Army tactical networks in the foreseeable future will not have abundant bandwidth to support the demand of network centric warfare. A similar situation has been encountered by Internet users in the past. Before the proliferation of broadband access networks, the most common way to access the Internet from average households was using dial-up services, which provides very low bit rate for data transport. This problem was generally referred to as first/last mile problem, and it was eventually resolved by the deployment of broadband access (cable, DSL, etc.) networks. Before the Internet service providers began to offer broadband access, they used several approaches to improve network performance as perceived by the users to increase their satisfaction. For example, one approach

was to enable transparent compression and decompression at both ends of bandwidth-constrained access links; the other was to install proxy and use caching to avoid having to access information provided by servers that connected to the Internet via slow links. Yet another was to host a content delivery network in their networks. These are good examples on how the first/last mile problem could be alleviated by different management approaches.

Although future Army networks also exhibit the same shortcoming, namely the lack of bandwidth at the network edge, there are fundamental differences between the tactical networks and the Internet in the past. First, the households were one hop away from the Internet, while nodes in the future tactical network could be many hops away. Second, the households were predominantly information retrievers, while nodes in the future tactical network could be both information retrievers and information providers. Third, households had a permanent, reliable connection to the Internet, while nodes in the future tactical network may have intermittent connectivity and need to contend for network resources.

3.2 Policy-based network management

Policy-based network management [Bhatia et al, 2000] promised the benefits of automating network management tasks and enabling flexible configuration and reconfiguration. In general, a policy-based management system works as follows. It allows network operators to enter network objectives as policies into the system, and ensures automatic enforcement of these policies so that no further manual action is required of the network operators. Once such policies are defined, they are automatically enforced by the management system. These capabilities provide network operators with very powerful tools to configure and control their network, and to re-configure their network in response to ever-changing network conditions, with the highest possible level of automation.

However, today's commercial network management and network planning tools were mostly designed for networks with abundant bandwidth and stable topologies. They are centralized for easy commercial deployment; they neither minimize bandwidth usage nor do they stress on survivability. These tools are ill-suited for military MANETs due to the differences in characteristics of MANETs and conventional networks. MANET management tools require self-healing and self-adapting capabilities because MANET conditions may change considerably anytime. MANETs must limit network management traffic because the limited bandwidth available should be used predominantly by application traffic; besides, they need to cope with unpredictable link quality and network connectivity.

3.3 Middleware

Middleware has been used as a means to provide a universal data exchange interface between heterogeneous systems. For example, CORBA [OMG, 2006] is a well-known example that has been adopted by the Internet community. Middleware hides the complexity of dealing with heterogeneous systems from the applications; at the same time, it provides a flexible function invocation mechanism with its broker architecture. Applications can retrieve needed information and obtain services provided by other applications without knowing a priori where the information is stored, what applications are providing the services and where they are located in the network. The mechanisms provided by middleware significantly simplify application development for heterogeneous environments.

Nevertheless, middleware that has been widely used for the Internet is not suitable for the future Army networks. The main reason is that some of the underlying assumptions made by today's middleware frameworks will not hold in the future Army networks: There is no guarantee that nodes providing services will always have connectivity to the network; network capacity will be much smaller than that of the Internet due to the use of MANETs in both WIN-T and FCS networks; and the strict client-server architecture does not offer the flexibility needed for the Army networks.

4. TRANSFORMING NETWORK MANAGEMENT

From the discussion in the previous sections, it should be clear that the future Army network needs to better manage its network resources. Further, existing state-of-the-art technologies are not readily applicable to the issues and challenges of the future networks. As a result, to transform network management for the future Army networks, research efforts are needed to enhance existing technologies in the areas of network operation automation, information dissemination management, and transparent communications adaptation. In addition, ground-breaking effort is needed in the areas of mission-oriented network operations, overarching policy coordination, and the integration of network management, information assurance, and information dissemination into a unified common architectural framework. Below we discuss recent research results, ongoing efforts, and major items requiring future work.

4.1 Recent research results

- DRAMA

In 2000, the U.S. Army CERDEC launched the Dynamic ReAddressing and Management for the Army (DRAMA) program, which was a five-year Science and

Technologies Objective (STO). Its main focus was on designing and developing a tool suitable for managing MANETs. It resulted in the creation of a network management tool that is distributed, agent-based, and policy-enabled [Chiang et al, 2005b]. This system provides the necessary self-healing and self-adaptive functionalities required for managing MANETs, and it can scale to manage a MANET with 500+ nodes [Chiang et al, 2006a]. The enforcement of policies by distributed intelligent agents allows the behavior of this management tool to autonomously adapt to dynamic network condition changes. The concept of operations of policy-based network management is shown in Fig. 2.

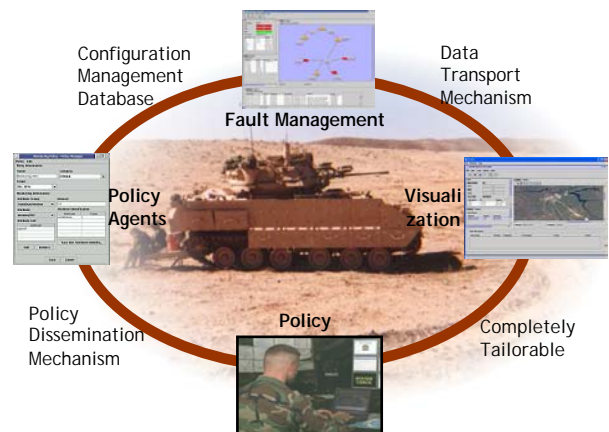


Fig. 2. The concept of operations of policy-based network management

DRAMA represents the state-of-the-art in automating MANET management, and it is currently being transitioned to the FCS network management system. By using a policy-based management tool like DRAMA, a network can autonomously adjust its behavior by implementing policies reflecting the commander's intention, thus greatly reducing the dependency on human administration and providing much better network resilience and reliability.

- Adaptive communications middleware

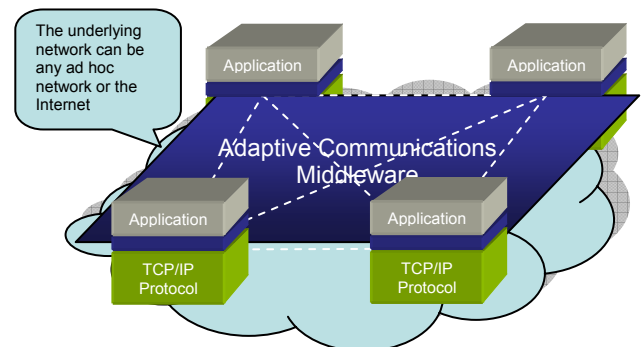


Fig. 3. The Concept of Adaptive Communications Middleware

To be able to adapt communications behavior to dynamic conditions, an important component of DRAMA was adaptive communications middleware that responds to network condition changes [Chiang et al, 2005a], as shown in Fig. 3. This allows autonomic tuning of communications performance. This middleware provides a generic application programming interface and can be used by applications other than DRAMA. It consists of a distribution layer and a transport layer. The rationale behind having these two layers in this middleware architecture is to keep the components interfacing with the DRAMA components and those interfacing with the network transport protocols completely separate. This design approach offers the following advantages:

- Since there is an interface between the distribution layer and the transport layer, it allows the middleware system to handle different distribution requirements with the most suitable network transport technologies on the fly. For example, if a new transport protocol can provide reliable transport similar to that provided by TCP, the middleware may use this new transport protocol instead of TCP under certain situations, as long as application communications requirements can still be satisfied.
- The separation of distribution and transport functionalities also realizes the concept of *delayed binding* [Maltz and Bhagwat, 1998]. This approach simplifies the application logic because the application delegates the communication identifier resolution responsibility to the middleware system. As a result, the distribution layer is responsible for resolving communication identifiers of the communication endpoints to their DNS representations, and the transport layer in turn maps the DNS representations to the network identifiers, which could be bundle identifiers in the context of Delay/Disruption Tolerant Networks [Farrell et al, 2006], a multicast group ID if there exists underlying multicast support, unicast and broadcast IP addresses, or a mix of all the above.

4.2 Ongoing efforts

- Mission-oriented network operations

Although the successful development of the DRAMA management tool shows that a big stride has been made in automating network management, policy-based management systems will require policies as input for them to function. The state of the art is that policies are specified by network administrators. Given that military missions could have different communications requirements and therefore they would require different management policies for the networks to function most effectively, the following question arises: *in the network planning process, can we automate the process of*

generating network management policies suitable for different types of military missions having their own communications requirements?

The complete automation of both network management and network planning based on specific mission needs is a major challenge. Our position is that automating the generation of network management policies in the network planning process is a necessity rather than a desirable feature. The specification of a suitable set of policies to manage dynamic MANETs is not trivial; besides, it is very difficult to validate the correctness and consistency of a large set of policies. Therefore, in addition to automating network management with policy control, we must also automate the generation of network management policies during the network planning process by taking into account the communications needs of the target mission.

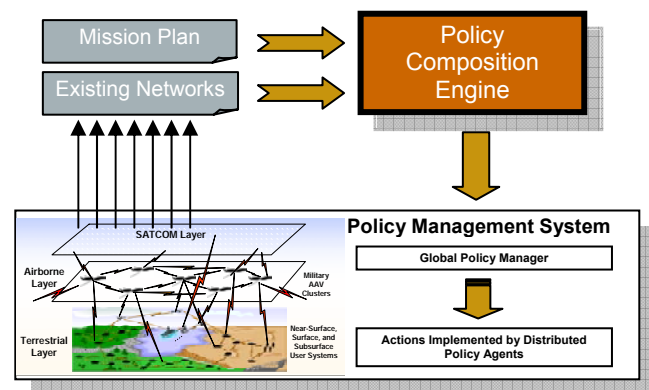


Fig. 4. Mission-driven Network Management Model

With guidance and support from the FCS BCT Technologies, U.S. Army CERDEC and Telcordia work together to investigate the issues involved in automating the generation of network management policies. This endeavor, codenamed 'DYMINiON' (*Dynamic Network Managers Integrating On-the-move Networks*), aims at identifying a promising direction towards automating the generation of network management policies [Chiang et al, 2006b]. By streamlining network planning with network management, we will further automate military network operations.

The ultimate goal of the DYMINiON effort is as follows: Given an arbitrary military mission, automatically generate policies as input to a policy-based network management system such that the system can implement the policies to ensure effective functioning of the network under all circumstances. DYMINiON is still ongoing work, which opens up a new direction for customizing network management based on mission needs. The high-level concept of mission-driven network management model is illustrated in Fig. 4.

We regard the DYMINiON work as a first crack at a very hard problem in network planning automation. The results obtained so far show that our approach is promising. On the other hand, we have identified more issues to address. For example, there is a tradeoff issue between the effectiveness of a plan and the computation time taken to automatically generate the plan. We have therefore redirected some of our attention from investigating possible alternatives at several module/algorithm decision points to reducing the computation time needed to generate a plan at the desired effectiveness level.

We also plan to tie our framework with other currently available planning tools. We believe that there is a need to come up with an overarching architectural framework such that tools geared towards network planning purposes can be integrated seamlessly.

4.3 Required future work

- Policy consistency across networks

To the best knowledge of the authors, DRAMA is the first distributed policy-based management system possessing the necessary properties for managing tactical networks. As the concept of policy-based management permeates into military networks, it is important to ensure that policies implemented by different network management systems will be coordinated to ensure there is no conflict between their policies. For example, QoS policies implemented by FCS and WIN-T must be consistent with each other to ensure that the assured quality of service will be obtained by applications when their traffic needs to transit across network boundaries. An overarching policy control architecture that can detect and resolve potential policy conflicts, and furthermore, automatically generate conflict-free policies across different network management systems, is needed.

- Smart information dissemination middleware

A content distribution system that can react to user demands, adapt to network conditions, and deliver information promptly will be invaluable to warfighters. It needs to appropriately address a varied set of requirements including availability, resilience, bandwidth overhead, security, authentication, and confidentiality. The major challenges lie in smooth performance degradation in the event of intermittent network connectivity and network congestion, and in the location of already-disseminated information in nearby nodes. Chances are that information dissemination services might be needed (and therefore requested) the most when the battle is fierce and network service quality is marginal. The goal is to build a content distribution system incorporating the capability of information dissemination, adaptive communications, and information warehousing.

- Automated network re-planning

In addition to furthering the research on automated network planning, it is also important to investigate the automation of network re-planning. Network re-planning is fundamentally different from network planning—network planning plans a network from the scratch while network re-planning focuses on addressing outstanding issues in the network. The goal of network planning is to take the assumed mission scenarios into account and come up with a network plan. However, the reality may deviate from the assumed scenarios for many reasons; in some situations, a network must be re-planned. Therefore, network re-planning is to deal with the issues that were not considered sufficiently by the original plan. The two essential differences between planning and re-planning are: (i) the modified plan should cause minimal impact to the ongoing communications; and (ii) the re-planning process should be able to address issues in real time or near real time.

- A common framework integrating information assurance, information dissemination and network management

Lastly, we foresee the need for integrating the functions of information assurance, information dissemination, and network management into a common framework. As of today, they are independent functions in the network. However, from the mission-oriented network operation viewpoint, these components need to be loosely coupled within one single system using policies to coordinate the behavior of individual functions. The idea is that the network needs to be managed as a whole such that it can deliver the highest possible performance to warfighters under any circumstances.

5. PATH FORWARD

Since policy-based management systems are being developed for the FCS and WIN-T programs to automate network management, we are already in the process of transforming network management for the future Army networks. However, transforming network management is not an easy task, as explained in the previous sections. The key elements in this transformation are automation and mission-orientation. We need to address the various technology gaps to accomplish the transformation.

Meanwhile, we also need to ensure that the developed technologies can be seamlessly integrated into the Army network in an incremental fashion. At CERDEC, an interoperability laboratory is currently being built to host network management systems at all echelons to test interoperability and performance. This laboratory will host a network test bed running various network management tools that will be connected according to the proposed future network architecture.

The test bed will be used to perform independent out-of-the-box testing to verify that these tools will meet their own requirements. CERDEC will act as the “honest broker” to ensure that these network management tools can perform as expected and check if there is any issue to be addressed. To facilitate the interoperability requirements testing, an XML schema is being defined to specify the relationships between different network management systems. This schema is network-neutral and therefore can be used for verifying the interoperability of network management tools across the military services. Testing of various focus areas can be conducted by describing the context and requirements using this XML schema, including network capacity, bandwidth usage, system scalability, etc. Such testing can identify and address issues before large-scale field testing and deployment. Lastly, this laboratory will also be used to test the interoperability of network management tools for the current force and those being built for the future force.

6. CONCLUSIONS

In this paper, we presented our vision of transforming network management for the future Army networks. We believe that in order to achieve the vision of network centric warfare, the philosophy of network management must transition from maintaining network operations to providing optimal communications services. We believe that this transformation will greatly enhance the performance of information access for the future war-fighting needs.

ACKNOWLEDGEMENT

We would like to thank PM FCS BCT Technologies for their continued guidance and support of the DYMINION research.

REFERENCES

- A. Agarwal and P.R. Kumar, 2004: Capacity Bounds for Ad hoc and Hybrid Wireless Networks. ACM SIGCOMM Computer Communications Review Volume 34, Number 3, ACM.
- R. Bhatia, J. Lobo, M. Kohli, 2000: Policy Evaluation for Network Management. INFOCOM 2000, Volume 3, IEEE, 1107–1116.
- R. Chadha, Y.-H. Cheng, C.-Y. J. Chiang, S. Li, G. Levin, and A. Poylisher, 2005a: DRAMA: A Distributed Policy-Based Mobile Ad Hoc Network Management System. Proc. of the 2005 Military Communications Conference (MILCOM 2005), Atlantic City, NJ, IEEE.
- R. Chadha Y.-H. Cheng, C.-Y. J. Chiang, S. Demers, P. Gopalakrishnan, L. Kant, S. Li, G. Levin, Y. Ling, and A. Poylisher, 2005b: DRAMA Performance and Scalability Analysis Report. A deliverable to the U.S. Army CERDEC.
- C.-Y. J. Chiang, R. Chadha, G. Levin, S. Li, and Y.-H. Cheng, 2005a: AMS: An Adaptive Middleware System for Ad hoc Networks. Proc. of the 2005 Military Communications Conference (MILCOM 2005), Atlantic City, NJ, IEEE.
- C.-Y. J. Chiang, R. Chadha, Y.-H. Cheng, S. Li, G. Levin, and A. Poylisher, 2005b: A Novel Software Agent Framework with Embedded Policy Control. Proc. of the 2005 Military Communications Conference (MILCOM 2005), Atlantic City, NJ, IEEE.
- C.-Y. J. Chiang, Y.-H. Cheng, S. Demers, P. Gopalakrishnan, L. Kant, R. Chadha, S. Li, G. Levin, A. Poylisher, Y. Ling, S. Newman, L. LaVergne, and R. Lo, 2006a: Performance analysis of DRAMA: A distributed policy-based system for MANET management. Proc. of the 2006 Military Communications Conference (MILCOM 2006), DC, IEEE.
- C.-Y. J. Chiang, R. Chadha, S. Newman, and R. Lo, 2006b: Toward Automation of Network Management and Planning for Future Tactical Networks. Proc. of the 2006 Military Communications Conference (MILCOM 2006), DC, IEEE.
- DoD, 2001: Department of Defense Report to Congress. [Available online at <http://www.dod.mil/nii/NCW/>]
- DoD, 2004: Global Information Grid. [Available online at http://akss.dau.mil/dag/Guidebook/IG_c7.2.asp]
- S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald, 2006: When TCP Breaks: Delay- and Disruption-Tolerant Networking. Internet Computing, vol. 10, no. 4, IEEE, 72-78.
- C. L. Fullmer and J.J. Garcia-Luna-Aceves, 1997: Solutions to Hidden Terminal Problems in Wireless Networks. Proc. Sigcomm 1997, ACM.
- JTRS JPEO, cited 2006: Joint Tactical Radio Systems. [Available online at <http://enterprise.spawar.navy.mil/body.cfm?type=c&category=27&subcat=60>]
- J. Li, C. Blake, D. S. J. De Couto, H. I. Lee, and R. Morris, 2001: Capacity of Ad Hoc Wireless Networks. Proc. Of MobiCom 2001, ACM.
- D. A. Maltz and P. Bhagwat, 1998: TCP Splicing for Application Layer Proxy Performance. IBM Research Report.
- OMG cited 2006: CORBA: Common Object Request Broker Architecture. [Available online at www.corba.org]
- PM FCS, cited 2006: Future Combat Systems. [Available online at <http://www.army.mil/fcs/>]
- PM WIN-T, cited 2006: Warfighter Information Network -Tactical (WIN-T). [Available online at <http://www.globalsecurity.org/military/systems/ground/win-t.htm>]